

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
29. August 2002 (29.08.2002)

PCT

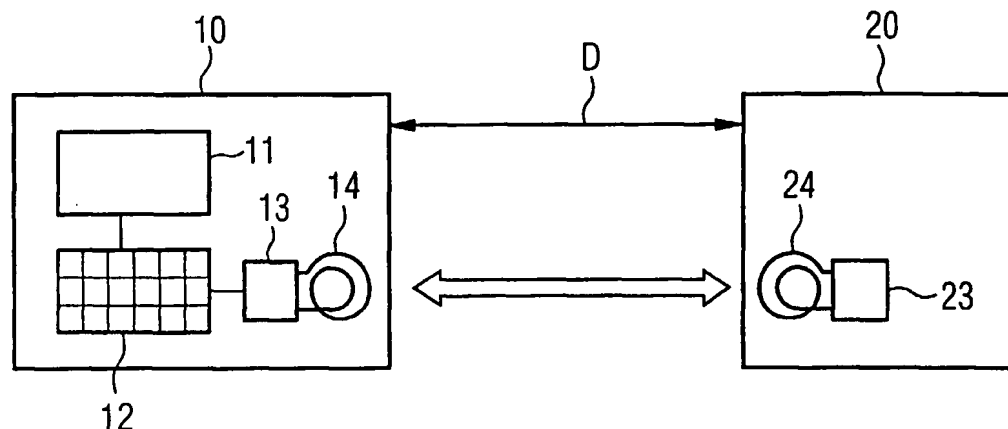
(10) Internationale Veröffentlichungsnummer
WO 02/067211 A1

- (51) Internationale Patentklassifikation⁷: **G07F 7/08, 7/10** (71) **Anmelder** (für alle Bestimmungsstaaten mit Ausnahme von US): **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).
- (21) Internationales Aktenzeichen: **PCT/DE01/04893**
- (22) Internationales Anmeldedatum: **21. Dezember 2001 (21.12.2001)** (72) **Erfinder; und**
- (75) **Erfinder/Anmelder** (nur für US): **HEILINGBRUNNER, Andrea** [DE/DE]; Malsenstr. 35, 80638 München (DE). **MAY, Christian** [DE/DE]; Stuntzstr. 19/V, 81677 München (DE).
- (25) Einreichungssprache: **Deutsch**
- (26) Veröffentlichungssprache: **Deutsch** (74) **Anwalt: EPPING HERMANN & FISCHER**; Ridlerstr. 55, 80339 München (DE).
- (30) Angaben zur Priorität: **101 08 819.1** **23. Februar 2001 (23.02.2001)** **DE** (81) **Bestimmungsstaaten (national)**: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR SECURELY HANDLING A DATA COMMUNICATION CONCERNING A FINANCIAL TRANSACTION

(54) **Bezeichnung:** VERFAHREN ZUR SICHEREN ABWICKLUNG EINER EIN GELDGESCHÄFT BETREFFENDEN DATENKOMMUNIKATION



(57) **Abstract:** The invention relates to a method for securely handling a data communication concerning a financial transaction between a portable data carrier and a terminal. The data carrier contains a data transmission interface, a display device, an input device and a means containing unequivocal, particularly personalised data. The terminal comprises a corresponding data transmission interface. According to the invention, a direct communication occurs between the data carrier and the terminal, at least when a data communication is established, in such a manner that an involuntary transmission of information is not possible because of the distance between the data support and the terminal.

(57) **Zusammenfassung:** Die Erfindung schlägt ein Verfahren zur sicheren Abwicklung einer ein Geldgeschäft betreffenden Datenkommunikation zwischen einem tragbaren Datenträger und einem Terminal vor. Der Datenträger enthält eine Datenübertragungsschnittstelle, eine Anzeigevorrichtung, eine Eingabevorrichtung und ein Mittel mit eindeutigen, insbesondere personalisierten Daten. Das Terminal weist eine korrespondierende Datenübertragungsschnittstelle auf. Es ist vorgesehen, daß zumindest beim Aufbau der Datenkommunikation eine direkte Kommunikation zwischen dem Datenträger und dem Terminal derart stattfindet, daß aufgrund der Distanz zwischen dem Datenträger und dem Terminal auch eine unbeabsichtigte Übertragung von Informationen an Dritte nicht möglich ist.

WO 02/067211 A1



(84) **Bestimmungsstaaten** (*regional*): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— mit internationalem Recherchenbericht

Beschreibung

Verfahren zur sicheren Abwicklung einer ein Geldgeschäft betreffenden Datenkommunikation

5

Die Erfindung betrifft ein Verfahren zur sicheren Abwicklung einer ein Geldgeschäft betreffenden Datenkommunikation zwischen einem Datenträger und einem Terminal.

- 10 Tragbare Datenträger in Form von personalisierten, mobilen Assistenten (PMA) finden eine immer größere Verbreitung in der Bevölkerung. PMAs weisen den Vorteil auf, daß sie klein, leicht und einfach zu bedienen sind.
- 15 Es ist daran gedacht, die häufig als elektronische Notizbücher oder Telefone genutzten Geräte auch als elektronische Geldbörse einzusetzen. Die Daten einer Kredit- oder Geldkarte könnten zu diesem Zweck in dem PMA gespeichert sein. Bei einem Bezahlvorgang können die Daten z.B. bei gleichzeitiger
- 20 Eingabe einer persönlichen Geheimnummer an eine Kasseneinrichtung übertragen und auf diese Weise die Zahlung abgewickelt werden.

- Angedacht ist auch, das Bezahlen per Handy über Short Message
- 25 Services (SMS), ein Bankkonto bei einer Bank und zugeteilte, für jede Transaktion unterschiedlich verwendete Pin-Codes zu realisieren.

- Voraussetzung für die sichere Abwicklung des Geldgeschäftes
- 30 zwischen dem tragbaren Datenträger und dem Terminal, z. B. einer Registrierkasse, ist, daß die Kommunikation tatsächlich zwischen diesen beiden Geräten aufgebaut und abgewickelt wird. Die Abwicklung im vorgenannten Sinne umfaßt dabei auch einen dritten Teilnehmer, z. B. eine Bank, die die tatsächlichen
- 35 Abbuchungen nach dem Entstehen der Kommunikation zwischen dem tragbaren Datenträger und dem Terminal vornimmt.

Die Aufgabe der Erfindung besteht darin, ein Verfahren der oben genannten Art anzugeben, das eine sichere Abwicklung eines Geldgeschäftes ermöglicht und dabei einen hohen Schutz vor Mißbrauch gewährleistet.

5

Diese Aufgabe wird mit den Merkmalen des Anspruchs 1 gelöst. Bevorzugte Ausgestaltungen des erfindungsgemäßen Verfahrens ergeben sich aus den abhängigen Ansprüchen.

- 10 Erfindungsgemäß wird ein Verfahren zur sicheren Abwicklung einer ein Geldgeschäft betreffenden Datenkommunikation zwischen einem tragbaren Datenträger, der eine Datenübertragungsschnittstelle, eine Anzeigevorrichtung, eine Eingabevorrichtung und ein Mittel mit eindeutigen, insbesondere perso-
- 15 nifizierten Daten enthält, und einem eine korrespondierende Datenübertragungsschnittstelle enthaltenden Terminal vorgeschlagen, wobei zumindest beim Aufbau der Datenkommunikation eine direkte Kommunikation zwischen dem Datenträger und dem Terminal derart stattfindet, daß aufgrund der Distanz zwischen dem Datenträger und dem Terminal auch eine unbeabsichtigte Übertragung von Informationen an Dritte nicht möglich ist.

- 25 Mit anderen Worten löst die Erfindung das Problem der sicheren Datenkommunikation durch den Aufbau einer kurzreichweitigen Verbindung zwischen dem tragbaren Datenträger und dem Terminal. Die kurzreichweitige Verbindung ist dabei weniger durch die Entfernung zwischen dem tragbaren Datenträger und dem Terminal definiert, als vielmehr dadurch, daß der Datenaustausch zwischen diesen beiden Geräten auf eine derartige Weise stattfindet, daß zum einen eine unbeabsichtigte Übertragung von Informationen an Dritte unmöglich ist und zum anderen auch ein gezieltes "Abhören" mit entsprechenden Geräten, welche sich innerhalb der Übertragungsstrecke zwischen
- 30 tragbarem Datenträger und Terminal befinden, nicht möglich ist.
- 35

Wird die Kommunikation zwischen dem tragbaren Datenträger und dem Terminal mittels kontaktlos ausgebildeter Schnittstellen erfolgen, so werden gemäß dem Gedanken der Erfindung induktive Übertragungssysteme verwendet, die lediglich im Bereich
5 weniger Millimeter oder Zentimeter miteinander kommunizieren können.

Im Falle einer kontaktbehafteten Schnittstelle ist von Haus aus sichergestellt, daß eine unbeabsichtigte Übertragung von
10 Informationen an Dritte nicht möglich ist.

Bei Verwendung einer Infrarot-Schnittstelle ist die Übertragungsreichweite so zu bemessen, daß eine Informationsübertragung lediglich zwischen dem Terminal und dem tragbaren Daten-
15 träger stattfindet. Je kürzer die Übertragungsstrecke gewählt wird, desto geringer ist die Wahrscheinlichkeit, daß durch eine Streuung des Infrarot-Strahls Informationen an einen Dritten übertragen werden können.

20 Eine weitere Möglichkeit zum Aufbau der Kommunikation besteht darin, einen Barcode einzulesen, der entweder in der Anzeigevorrichtung des Datenträgers dargestellt und durch das Terminal eingelesen wird oder der von dem Terminal dargestellt und durch eine Lesevorrichtung des Datenträgers eingelesen wird.
25 Im ersten Fall könnten die an Kassensystemen mittlerweile üblichen Barcode-Lesegeräte zur Erfassung des in der Anzeigevorrichtung dargestellten Barcodes verwendet werden. In der Regel ist das Auslesen eines Barcodes nur dann möglich, wenn ein geringer Abstand zwischen diesem und dem entsprechenden
30 Lesegerät besteht.

Das der Erfindung zugrundeliegende Prinzip besteht folglich darin, zum einen eine direkte Kommunikation zwischen dem Datenträger und dem Terminal vorzusehen und diese Kommunikation
35 zum anderen derart durchzuführen, daß aufgrund der physikalischen Gegebenheiten auch eine unbeabsichtigte Übertragung von Informationen an Dritte unterbunden wird.

Wesentlich bei der kurzreichweitigen Kommunikation ist, daß die Übertragungsleistung hinreichend rasch mit einem zunehmenden Abstand D zwischen dem tragbaren Datenträger 10 und dem Terminal 20 abnimmt. Hierdurch ergibt sich eine physikalische Abschirmung gegenüber anderen Sende-Empfangsstationen.

Es ist weiterhin vorgesehen, den Aufbau der Kommunikation zwischen dem Datenträger und dem Terminal zunächst unverschlüsselt vorzunehmen, anschließend einen Schlüssel auszutauschen, der für die weitere, verschlüsselte Kommunikation verwendet wird.

Die verschlüsselte Kommunikation kann dabei entweder auf einem symmetrischen Verschlüsselungsverfahren, oder auf einem Verfahren, das mit Public/Private Keys arbeitet, beruhen.

Die verschlüsselte Kommunikation kann weiterhin direkt zwischen dem Datenträger und dem Terminal stattfinden. Ebenso ist es denkbar, nachdem eine verschlüsselte Kommunikation aufgebaut wurde, über eine dritte Instanz, z. B. eine Bank, zu kommunizieren.

Der Schlüssel kann erfindungsgemäß über die Datenübertragungsschnittstelle oder über die Anzeigevorrichtung des Datenträgers an das Terminal übertragen werden. Vorzugsweise beinhaltet der Schlüssel die eindeutigen Daten des Datenträgers, z.B. seine Seriennummer. Er kann auch eine über die Eingabevorrichtung eingegebene Zeichenfolge beinhalten oder durch diese gebildet sein. Wird der Schlüssel über die Anzeigevorrichtung des Datenträgers an das Terminal übertragen, so bietet sich hierfür der eingangs genannte Barcode an. Dieser beinhaltet dann bereits alle Informationen des Schlüssels.

Weiterhin ist vorgesehen, daß nach dem Austausch des Schlüssels ein das Geldgeschäft betreffender Betrag zwischen dem Datenträger und dem Terminal ausgetauscht wird, wobei zur

Vervollständigung des Geldgeschäfts eine Bestätigung über die Eingabevorrichtung des Datenträgers notwendig ist.

Die Eingabevorrichtung kann hierbei in einer Tastatur oder
5 lediglich in einem hierfür vorgesehenen Knopf, Taste oder
Schalter bestehen. Die Bestätigung erfolgt vorzugsweise erst
dann, wenn dem Nutzer in der Anzeigevorrichtung des Datenträ-
gers der abzubuchende Betrag angezeigt wird. Stimmt dieser
mit dem vereinbarten Betrag überein, so wird er das Geldge-
10 schäft durch Betätigung der Eingabevorrichtung bestätigen.
Zeigt die Anzeigevorrichtung jedoch einen anderen Betrag als
den ausgemachten Geldbetrag an, so kommt durch eine nicht
durchgeführte Bestätigung über die Eingabevorrichtung das
Geldgeschäft nicht zustande. Alternativ ist denkbar, das
15 Geldgeschäft durch Drücken einer dafür vorgesehenen Taste der
Eingabevorrichtung zu verwerfen.

In einer anderen Variante ist vorgesehen, daß vor dem Aufbau
der Datenkommunikation zwischen dem Datenträger und dem Ter-
20 minal über die Eingabevorrichtung ein das Geldgeschäft be-
treffender Betrag in den Datenträger eingegeben und über die-
se bestätigt wird und erst anschließend die Datenkommunikati-
on in oben beschriebener Weise aufgebaut wird. Nach dem Auf-
bau der Datenkommunikation wird folglich der von dem Nutzer
25 in den tragbaren Datenträger eingegebene Betrag an das Termi-
nal übertragen. Ein möglicherweise falsch berechneter Betrag
ist dann auf das Verschulden des Nutzers zurückzuführen.

Die Erfindung und deren Vorteile wird anhand der nachfolgen-
30 den Figur näher erläutert.

Die Figur 1 zeigt einen tragbaren Datenträger 10 und ein Ter-
minal 20, mit denen das erfindungsgemäße Verfahren zur siche-
ren Abwicklung einer ein Geldgeschäft betreffenden Datenkom-
35 munikation durchgeführt werden kann. Der Datenträger 10 weist
zu diesem Zweck eine Anzeigevorrichtung 11, eine Eingabevor-
richtung 12 sowie eine Datenübertragungsschnittstelle 14 auf,

die mit einem Mittel 13 mit eindeutigen, insbesondere personifizierte Daten verbunden ist. Die Datenübertragungsschnittstelle 14 ist im vorliegenden Fall als Spule aufgeführt. Die Datenkommunikation mit dem Terminal 20 erfolgt somit auf kontaktlose, induktive Weise. Das Mittel 13 ist vorzugsweise als integrierte Schaltung ausgebildet. Diese kann fest in dem tragbaren Datenträger vorgesehen sein, sie kann jedoch auch in einer in den Datenträger einschiebbaren Datenträgerkarte (z. B. SIM-Karte oder Chipkarte) enthalten sein. In diesem Fall ist diese über entsprechend ausgebildete Kontakte mit der Datenübertragungsschnittstelle 14 sowie der Anzeige- bzw. Eingabevorrichtung 12 verbunden.

In entsprechender Weise weist das Terminal 20 eine zu der Datenübertragungsschnittstelle 14 korrespondierend ausgebildete Datenübertragungsschnittstelle 24 auf, welche gleichfalls mit einer integrierten Schaltung 23 verbunden ist. Bei dem Terminal 20 kann es sich beispielsweise um handelsübliche Registrierkassen, die in Supermärkten und Kaufhäusern eingesetzt werden, handeln.

Anstatt der als Spulen ausgebildeten Datenübertragungsschnittstellen könnten jeweils auch Kontakte oder optische Übertragungselemente, bestehend aus einem Sender und einem Empfänger, vorgesehen sein.

Zum Aufbau einer Kommunikation, die zunächst unverschlüsselt stattfindet, werden der tragbare Datenträger 10 und das Terminal 20 derart zueinander angeordnet, daß auf einer kurzreichweitigen Verbindung eine Kommunikation stattfinden kann. Im Falle einer induktiven Übertragung beträgt diese kurzreichweitige Verbindung nur wenige Millimeter oder Zentimeter. Der tragbare Datenträger 10 muß somit mit seiner Datenübertragungsschnittstelle annähernd auf das Terminal 20 aufgelegt werden. Hierdurch ist es nicht möglich oder zumindest mit hoher Wahrscheinlichkeit ausgeschlossen, daß eine unbeabsichtigte Übertragung von Informationen an Dritte erfolgt.

Dies ist insbesondere deshalb wichtig, da die Kommunikation, wie oben beschrieben, zunächst unverschlüsselt erfolgt. Nach dem Aufbau der Kommunikation wird ein Schlüssel zwischen dem tragbaren Datenträger und dem Terminal ausgetauscht, wodurch
5 im Anschluß eine verschlüsselte Kommunikation stattfinden kann. Diese kann entweder weiterhin direkt zwischen den beiden Geräten stattfinden oder aber über eine dritte Instanz, z. B. eine Bank, abgewickelt werden.

10 Ist die dritte Instanz, z. B. eine Bank, an der Datenkommunikation beteiligt, so kann von einem bei dieser geführten Konto der auszutauschende Geldbetrag ab- oder aufgebucht werden. Es ist jedoch auch denkbar, daß der tragbare Datenträger entsprechend dem Prinzip der Geldkarte einen Speicher mit einem
15 darin abgelegten Geldbetrag beinhaltet. Mit jeder ein Geldgeschäft betreffenden Datenkommunikation wird dann der jeweilige Betrag auf- oder abgebucht.

Das Auf- oder Abbuchen eines Geldbetrages zwischen dem Datenträger und dem Terminal, evtl. unter Zuhilfenahme der oben
20 genannten dritten Instanz, auszutauschen, wobei vor dem Abschluß des Geldgeschäftes eine Bestätigung durch den Besitzer des Datenträgers erfolgen kann. Beispielsweise kann diesem der abzubuchende Geldbetrag in der Anzeigevorrichtung 11 angezeigt werden. Ist der Geldbetrag korrekt, so kann der Nutzer diesen über die Eingabevorrichtung 12, bei der es sich um
25 eine Tastatur oder auch nur um einen einzelnen Knopf oder Schalter handeln kann, zu bestätigen. Findet eine derartige Bestätigung nicht statt, so entspricht dies einem Abbruch des
30 Geldgeschäftes.

Alternativ ist es möglich, in den tragbaren Datenträger 10 über die Eingabevorrichtung 12 einen Geldbetrag einzugeben und über die Eingabevorrichtung 12 zu bestätigen. Der Geldbetrag ist somit zunächst in der integrierten Schaltung gespeichert.
35 Nach dem Aufbau einer Datenkommunikation zu dem Terminal 20 und einem anschließenden Schlüsselaustausch findet die

Übertragung der in der integrierten Schaltung 13 gespeicherten Daten zu dem Terminal oder der dritten Instanz statt. Von dieser kann bestätigt werden, daß der Geldbetrag erhalten wurde. Anschließend kann der Geldbetrag entweder von dem

5 Speicher in dem tragbaren Datenträger 10 oder von einem Konto bei der dritten Instanz abgebucht werden.

Bezugszeichenliste

	10	Datenträger
	11	Anzeigevorrichtung
5	12	Eingabevorrichtung
	13	integrierte Schaltung
	14	Datenübertragungsschnittstelle
	20	Terminal
	23	integrierte Schaltung
10	24	Datenübertragungsschnittstelle
D		Abstand

Patentansprüche

1. Verfahren zur sicheren Abwicklung einer ein Geldgeschäft
betreffenden Datenkommunikation zwischen einem tragbaren Da-
5 tenträger (10), der eine Datenübertragungsschnittstelle (14),
eine Anzeigevorrichtung (11), eine Eingabevorrichtung (12)
und ein Mittel mit eindeutigen, insbesondere personifizierten
Daten (13) enthält, und einem eine korrespondierende Daten-
übertragungsschnittstelle (24) enthaltenden Terminal (20), wo-
10 bei zumindest beim Aufbau der Datenkommunikation eine direkte
Kommunikation zwischen dem Datenträger (10) und dem Terminal
(20) derart stattfindet, daß aufgrund der Distanz zwischen
dem Datenträger und dem Terminal (20) auch eine unbeabsich-
tigte Übertragung von Informationen an Dritte nicht möglich
15 ist.

2. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t, daß
der Aufbau der Kommunikation zwischen dem Datenträger (10)
20 und dem Terminal (20) zunächst unverschlüsselt erfolgt, an-
schließend ein Schlüssel ausgetauscht wird, der für die wei-
tere, verschlüsselte Kommunikation verwendet wird.

3. Verfahren nach Anspruch 2,
25 d a d u r c h g e k e n n z e i c h n e t, daß
der Schlüssel über die Datenübertragungsschnittstelle (14)
oder über die Anzeigevorrichtung (11) des Datenträgers (10)
an das Terminal (20) übertragen wird.

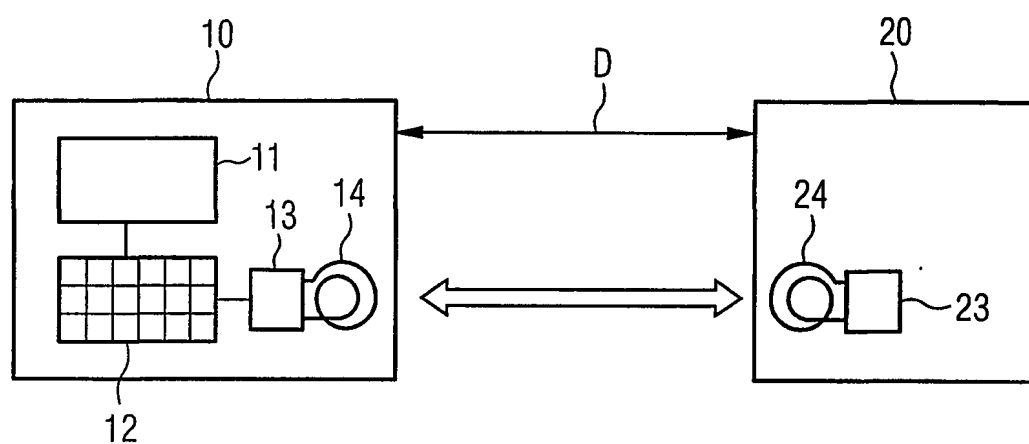
30 4. Verfahren nach Anspruch 2 oder 3,
d a d u r c h g e k e n n z e i c h n e t, daß
der Schlüssel eine über die Eingabevorrichtung (12) eingege-
bene Zeichenfolge beinhaltet oder durch diese gebildet ist.

35 5. Verfahren nach Anspruch 2 oder 3,
d a d u r c h g e k e n n z e i c h n e t, daß

der Schlüssel eindeutige Daten des Datenträgers (10) beinhaltet.

6. Verfahren nach einem der vorhergehenden Ansprüche,
5 d a d u r c h g e k e n n z e i c h n e t, daß
der Aufbau der Kommunikation mit einer als optisch, kontakt-
behafteten oder kontaktlos ausgebildeten Schnittstelle (14,
24) erfolgt.
- 10 7. Verfahren nach einem der Ansprüche 1 bis 5,
d a d u r c h g e k e n n z e i c h n e t, daß
der Aufbau der Kommunikation durch Einlesen eines Barcodes
erfolgt, der entweder in der Anzeigevorrichtung (11) des Da-
15 tenträgers (10) dargestellt und durch das Terminal (20) ein-
gelesen wird oder der von dem Terminal (20) dargestellt und
durch eine Leseeinrichtung des Datenträgers (10) eingelesen
wird.
- 20 8. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, daß
nach dem Austausch des Schlüssels ein das Geldgeschäft be-
treffender Betrag zwischen dem Datenträger (10) und dem Ter-
minal (20) ausgetauscht wird, wobei zur Vervollständigung des
Geldgeschäfts eine Bestätigung über die Eingabevorrichtung
25 (12) des Datenträgers (10) notwendig ist.
- 30 9. Verfahren nach einem der Ansprüche 1 bis 7,
d a d u r c h g e k e n n z e i c h n e t, daß
vor dem Aufbau der Datenkommunikation zwischen dem Datenträ-
ger (10) und dem Terminal (20) über die Eingabevorrichtung
(12) ein das Geldgeschäft betreffender Betrag in den Daten-
träger (10) eingegeben und über diesen bestätigt wird und
erst anschließend die Datenkommunikation aufgebaut wird.

1/1



INTERNATIONAL SEARCH REPORT

onal Application No
PCT/DE 01/04893

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 980 053 A (CITIBANK NA) 16 February 2000 (2000-02-16) paragraphs '0038!', '0045! paragraph '0058! - paragraph '0060! paragraphs '0077!', '0078!', '0090! ---	1,6-9
A	WO 99 39476 A (CERTICOM CORP ; VADEKAR ASHOK V (CA); GALLANT ROBERT P (CA); LAMBER) 5 August 1999 (1999-08-05) page 3, line 16 -page 5, line 25 ---	1,2,6
A	EP 1 017 029 A (FUJITSU LTD) 5 July 2000 (2000-07-05) paragraph '0059! - paragraph '0067! paragraph '0091! - paragraph '0096! claim 1 --- -/--	1-4,6,9

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

15 May 2002

Date of mailing of the international search report

27/05/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Bocage, S

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 01/04893

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 955 961 A (WALLERSTEIN ROBERT S) 21 September 1999 (1999-09-21) figures 2,7 column 5, line 22 -column 6, line 2 column 9, line 49 - line 60 ----	1-7,9
A	WO 98 25371 A (WANG YNJIUN) 11 June 1998 (1998-06-11) page 7, line 8 -page 8, line 4 page 13, line 26 -page 14, line 31 figures 5C,6A ----	1,2,6
A	WO 00 74008 A (TAIEB BAILLIE THIERRY) 7 December 2000 (2000-12-07) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 01/04893

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0980053	A	16-02-2000	AU 732373 B2	26-04-2001
			AU 4353099 A	16-03-2000
			EP 0980053 A2	16-02-2000
			JP 2000200319 A	18-07-2000
WO 9939476	A	05-08-1999	AU 2145999 A	16-08-1999
			CA 2320221 A1	05-08-1999
			WO 9939476 A1	05-08-1999
			EP 1050134 A1	08-11-2000
			JP 2002502186 T	22-01-2002
EP 1017029	A	05-07-2000	JP 2000184085 A	30-06-2000
			EP 1017029 A2	05-07-2000
US 5955961	A	21-09-1999	US 5585787 A	17-12-1996
WO 9825371	A	11-06-1998	US 5917913 A	29-06-1999
			AU 5383198 A	29-06-1998
			US 6282656 B1	28-08-2001
			WO 9825371 A1	11-06-1998
			US 6175922 B1	16-01-2001
			US 2002023215 A1	21-02-2002
WO 0074008	A	07-12-2000	FR 2771533 A1	28-05-1999
			WO 0074008 A1	07-12-2000
			AU 3832199 A	18-12-2000

INTERNATIONALER RECHERCHENBERICHT

nationales Aktenzeichen

PCT/DE 01/04893

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G07F7/08 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RESEARCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G07F G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 980 053 A (CITIBANK NA) 16. Februar 2000 (2000-02-16) Absätze '0038!, '0045! Absatz '0058! - Absatz '0060! Absätze '0077!, '0078!, '0090! ---	1, 6-9
A	WO 99 39476 A (CERTICOM CORP ; VADEKAR ASHOK V (CA); GALLANT ROBERT P (CA); LAMBER) 5. August 1999 (1999-08-05) Seite 3, Zeile 16 -Seite 5, Zeile 25 ---	1, 2, 6
A	EP 1 017 029 A (FUJITSU LTD) 5. Juli 2000 (2000-07-05) Absatz '0059! - Absatz '0067! Absatz '0091! - Absatz '0096! Anspruch 1 --- -/--	1-4, 6, 9

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

G Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

15. Mai 2002

Absendedatum des internationalen Recherchenberichts

27/05/2002

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Bocage, S

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 955 961 A (WALLERSTEIN ROBERT S) 21. September 1999 (1999-09-21) Abbildungen 2,7 Spalte 5, Zeile 22 -Spalte 6, Zeile 2 Spalte 9, Zeile 49 - Zeile 60 -----	1-7,9
A	WO 98 25371 A (WANG YNJIUN) 11. Juni 1998 (1998-06-11) Seite 7, Zeile 8 -Seite 8, Zeile 4 Seite 13, Zeile 26 -Seite 14, Zeile 31 Abbildungen 5C,6A -----	1,2,6
A	WO 00 74008 A (TAIEB BAILLIE THIERRY) 7. Dezember 2000 (2000-12-07) -----	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 01/04893

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0980053	A	16-02-2000	AU 732373 B2	26-04-2001
			AU 4353099 A	16-03-2000
			EP 0980053 A2	16-02-2000
			JP 2000200319 A	18-07-2000
WO 9939476	A	05-08-1999	AU 2145999 A	16-08-1999
			CA 2320221 A1	05-08-1999
			WO 9939476 A1	05-08-1999
			EP 1050134 A1	08-11-2000
			JP 2002502186 T	22-01-2002
EP 1017029	A	05-07-2000	JP 2000184085 A	30-06-2000
			EP 1017029 A2	05-07-2000
US 5955961	A	21-09-1999	US 5585787 A	17-12-1996
WO 9825371	A	11-06-1998	US 5917913 A	29-06-1999
			AU 5383198 A	29-06-1998
			US 6282656 B1	28-08-2001
			WO 9825371 A1	11-06-1998
			US 6175922 B1	16-01-2001
			US 2002023215 A1	21-02-2002
WO 0074008	A	07-12-2000	FR 2771533 A1	28-05-1999
			WO 0074008 A1	07-12-2000
			AU 3832199 A	18-12-2000